

IN THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the Application:

LISTING OF CLAIMS:

1 - 2. (Cancelled)

3. (Currently amended) The system proxy server according to claim 1, 25,
wherein said content-data file includes static content.

4. (Currently amended) The system proxy server according to claim 1, 25,
wherein said content-data file includes dynamic content.

5. (Currently amended) The system proxy server according to claim 1, 25,
wherein said communication means includes a secure transform configured to
encrypt and encapsulate encapsulating said content into a message encrypting
said received data block is performed as a function of a shared session ID secret
shared between said proxy server and said client machine is configured to extract
said content from said message.

6. (Currently amended) The system proxy server according to claim 1, 25,
wherein said proxy system server further includes a user interface, configured to
facilitate creation and editing of said access policies and said usage policies
policy and association of said access policies and said usage policies policy with
said content data file.

7 - 10. (Cancelled)

11. (Currently amended) The method of claim 9, 20, wherein said content data file includes static content.

12. (Currently amended) The method of claim 9, 20, wherein said content data file includes dynamic content.

13. (Currently amended) The method of claim 9, 20, wherein said communicating is accomplished using a communication means that includes a secure transform, including encrypting and encapsulating said content into a message encrypting said received data block is performed as a function of a shared session ID and said client device is configured to extract said content from said message secret shared between said proxy server and said client machine.

14. (Currently amended) The method of claim 9, 20, wherein said proxy system further server includes a user interface and step A include the method further includes creating and/or editing said access policies and said usage policies policy and associating said access policies and said usage policies policy with said content data file using said user interface.

15 - 16. (Cancelled)

17. (Currently amended) The system proxy server according to claim 4-25; wherein the access control module is further configured to encrypt each data block of the content data file is encrypted independently, using a unique initialization vector for each data block and one or more encryption/decryption keys; and

wherein the one or more communication means also provide the one or more encryption/decryption keys are also provided to said client device machine.

18. (Cancelled)

19. (Currently amended) The method of claim 9-20 wherein the method further comprises:

encrypting each data block of the content-data file independently, using a unique initialization vector for each data block and one or more encryption/decryption keys; and

communicating said one or more encryption/decryption keys to said client ~~device associated with said one or more user and/or client device identification machine.~~

20. (Previously Presented) A method performed by a proxy server, the method comprising:

receiving, over a first network connection, a Network File System (NFS) based request from a client machine for a data block of a data file from a remote network attached storage system, the request having an associated user, the data block having a fixed preconfigured size associated with the data file;

requesting, from an authentication server, an access policy associated with the associated user;

receiving, from the authentication server, the access policy associated with the associated user;

determining, from the access policy associated with the associated user and metadata associated with the data file, the metadata being stored on the remote network attached storage system, if the associated user has the authority to access the data file; and

if the associated user has the authority to access the data file, then:

establishing a set of usage rights based on the access policy associated with the associated user and the metadata associated with the data file;

requesting, over a second network connection, from the network attached storage system, the data block of the data file;

receiving, over the second network connection, from the network attached storage system, the data block of the data file;

encrypting the received data block, such that only an authorized client module executing on the client machine by the associated user can decrypt the encrypted received data block;

encapsulating within a packet:

the encrypted received data block; and

the established set of usage rights; and

sending, over a secure channel, the packet to the client machine such that only the authorized client module can access the encrypted received data block and only when such access is in accordance with the established set of usage rights, said authorized client module running transparently to the associated user, logically interposed between an application layer and an operating system kernel layer.

21. (Previously Presented) A method as in claim 20 wherein the established set of usage rights includes one or more access restrictions, each usage restriction including:

a restriction type; and

a set of parameters associated with the restriction type.

22. (Previously Presented) A method as in claim 21 wherein the restriction type indicates that data from the encrypted received data block may only be e-mailed to recipients listed within the set of parameters.

23. (Previously Presented) A method as in claim 20 wherein the access policy associated with the associated user includes a set of access conditions, each access condition including:

a condition type; and

a set of parameters associated with the condition type.

24. (Currently amended) A method as in claim 23 wherein the condition type indicates that the associated user only has the authority to access the data file when ~~the-a~~ a clock time falls between a first value listed in a first parameter of the set of parameters and a second value listed in a second parameter of the set of parameters.

25. (New) A proxy server, comprising:

processing circuitry; and
network communications circuitry;
the processing circuitry and network communications circuitry being operative together to perform a method including:
receiving, over a first network connection, a Network File System (NFS) based request from a client machine for a data block of a data file from a remote network attached storage system, the request having an associated user, the data block having a fixed preconfigured size associated with the data file;
requesting, from an authentication server, an access policy associated with the associated user;
receiving, from the authentication server, the access policy associated with the associated user;
determining, from the access policy associated with the associated user and metadata associated with the data file, the metadata being stored on the remote network attached storage system, if the associated user has the authority to access the data file; and
if the associated user has the authority to access the data file, then:
establishing a set of usage rights based on the access policy associated with the associated user and the metadata associated with the data file;

requesting, over a second network connection, from the network attached storage system, the data block of the data file;

receiving, over the second network connection, from the network attached storage system, the data block of the data file;

encrypting the received data block, such that only an authorized client module executing on the client machine by the associated user can decrypt the encrypted received data block;

encapsulating within a packet:

the encrypted received data block; and

the established set of usage rights; and

sending, over a secure channel, the packet to the client machine such that only the authorized client module can access the encrypted received data block and only when such access is in accordance with the established set of usage rights, said authorized client module running transparently to the associated user, logically interposed between an application layer and an operating system kernel layer.

26. (New) A proxy server as in claim 25 wherein the established set of usage rights includes one or more access restrictions, each usage restriction including:

a restriction type; and

a set of parameters associated with the restriction type.

27. (New) A proxy server as in claim 26 wherein the restriction type indicates that data from the encrypted received data block may only be e-mailed to recipients listed within the set of parameters.

28. (New) A proxy server as in claim 25 wherein the access policy associated with the associated user includes a set of access conditions, each access condition including:

a condition type; and

a set of parameters associated with the condition type.

29. (New) A proxy server as in claim 28 wherein the condition type indicates that the associated user only has the authority to access the data file when a clock time falls between a first value listed in a first parameter of the set of parameters and a second value listed in a second parameter of the set of parameters.